International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Efficient Cryptographic Method in Wireless Sensor Networks for Iot Healthcare System

Sangeetha Komandur[1*], Sameena Shaik[2],

Submitted: 28/01/2024 **Revised**: 06/03/2024 **Accepted**: 14/03/2024

Abstract: The open, large-scale, as well as resource-constrained atmosphere of wireless sensor networks (WSNs) continues to pose important issues in relations of efficiency, energy consumption as well as security. The security as well as effectiveness of WSNs may be enhanced with the help of several lightweight cryptographic algorithms that use reasonable amounts of energy and resources. Nevertheless, there are still issues with their adaptability, authentication, Key Management(KM) along with power resource management procedures. This study presents lightCrypt, an automated LightWeight Cryptographic(LWC) system for WSNs, which aims to solve these concerns. The proposed strategy proposes a flexible, LWC approach to regulate the difficulty of the encryption(EP) by automatically selecting cryptographic parameters depending on the current resource availability of individually sensor node to encrypt the data. To further ensure safe communication and key/data sharing across WSN nodes, a novel lightweight KM as well as authentication mechanism is developed. An evaluation of the proposed lightCrypt scheme was conducted. In comparison to alternative cyphers that employ set EP parameters, the findings show that the proposed technique significantly improves throughput, EP time, packet delivery ratio along with end to end delay. The lightCrypt system is secure and can withstand brute-force, eavesdropping, man-in-the-middle as well as replay attacks, according to the security study.

Keywords: *Datasets, Internet of Things (IoT), EP, Decryption(DP), WSNs, Key*

1. Introduction

Because of the limited control of resources across the vast IoT connection zone, WSNs are susceptible to attacks. There are a number of shared characteristics across the small sensor nodes, such as the ability to detect and store energy, temperature, and medical data in IoT devices [1]. There will be a dramatic increase in the use of health monitoring sensors within the next decade. Many individuals nowadays use smartwatches as a health tracker. The IoT, WSNs, along with cloud ideas all promote sensor use [2].

With health cloud storage, doctors and other medical professionals always have access to patient records. Consequently, patient monitoring and treatment cannot proceed without secure data communication. Furthermore, safeguards should be put in place to prevent data abuse and tampering when storing the patient's information, since it may be readily track by other devices. Owing to the restricted number of devices connected to the IoT, using high-level cryptographic techniques to encrypt data becomes even more challenging [3]. The patient's private information might be at risk if the potential devices are hacked due to their internet connectivity. Security has therefore become a vital element of today's computing environment due to the widespread environment of IoT entities in over-all as well as IoT-based HealthCare(HC) in specific. This study details the method for encrypting private health data during transmission in an IoT setting using a wireless network. With the goal of preserving users' anonymity and security as they engage in online activities, the algorithm identifies data that cannot be disclosed [4].

Some design flaws make the existing protocols vulnerable to security risks, including user and sensor impersonation attacks. Using lightweight elliptic curve cryptography (ECC), this paper suggests a new architecture for MWSNs and creates an appropriate authenticated key formation mechanism for it. With the suggested authentication mechanism, the protocols' security holes are filled. The Burrows-Abadi-Needham (BAN) reasoning is recycled to show that the protocol is accurate. Additional analysis has shown that the protocol is harmless against known security attacks. Furthermore, the protocol is designed in Verilog Hardware Description Language (HDL), along with its functioning is tested using the Altera Quartus II simulation tool for FPGA implementation [5]. This concentrates on WSN applications, security needs, various attacks and responses, as well as current problems and difficulties. Virtualization, data storage, and Software Defined Networking (SDN) integration into WSNs are further defined using a new set of difficulties [6].

A fast and trustworthy authentication method for the HealthCare System(HCS) that is compatible with devices that have limited power and bandwidth. This method

[1,2]*Lecturer*
Department Of Computer Science, College Of Computer Science & Information Technology, Jazan Univeristy,
Jazan-45142, SaudiArabia
[1]** Corresponding Author Email: skomandur@jazanu.edu.sa*
[2]*sabdualoheed@jazanu.edu.sa*

usages random numbers in its place of difficult EP and DP to decrease calculation time along with energy. According to the results of the performance and security study, the solution extends the life of the network and is superior to its competitors in terms of computing costs, communication costs, and security [7]. A safe pairing-free certificateless signcryption method for routine in large-scale HCS. In contrast to earlier congruent signcryption systems, it evaluates the efficacy of method. An official security proof of scheme's indistinguishability against adaptively selected cypher text attacks and unforgeability against adaptively chosen message assaults is provided by the random oracle model [8].

Effective resolution of the security difficulties related to strong EP methods, KM, authentication, and trust management is essential. A lightweight security strategy is required, one that accounts for the aforementioned four considerations. In order to dynamically trade-off EP power with regard to wireless sensor limits as well as available resources, a lightweight EP system is proposed in this study. The following is an overview of the main points made by this work:

a. LightCrypt, an automated, along with lightweight EP method, is proposed for WSN networks. Using a lightweight EP approach in commerce with cryptographic parameters in resource-constrained sensor nodes, the proposed system ensures high security. A lightweight and authentication technique is also proposed for use in WSNs to facilitate safe connection establishment, data sharing, and symmetric key exchange.

b. The EP process's complexity may be dynamically controlled by the proposed approach according to the resources that each sensor node presently has.

c. Finally, the research provides our scheme's security and performance evaluations.

The remaining tasks are set up: The second section provides a literature review on relevant topics, including the use of WSN in IoT HCS algorithms. In Section 3, go over the model that the Cryptographic Method suggests. The study is concluded with Section 5, which includes the references and Section 4, which gives the results gained and the dataset utilized for simulation.

2. Recent works for Research.

Jabeen et al. [9], introduced a nanosensors as part of an intelligent HCS's real-time data collection and transmission system. A number of current methods have limitations, and there are major concerns with time consumption and other forms of attacks. This work suggests a genetically based EP approach to safeguarding data transferred over a wireless channel by means of sensors, so escape unpleasant data transmission environments.

Huang et al. [10] described the privacy as well as information security remain major concerns in the ever-expanding realm of e-/m-healthcare. The creation of a HCS framework addresses these issues. An extensive WSNs architecture receives medical data from WBANs, processes it, and then publishes it into wireless personal area networks (WPANs) via a gateway. An expert system that can automatically analyse and report the results of encrypted medical data is also part of HES, along with the HEBM (Homomorphic EP Based on Matrix) scheme for privacy as well as the GSRM (Groups of Send-Receive Model) method for key distribution.

Gardasevic et al. [11], provided a critical evaluation of emerging IoT connection protocols and technologies as they pertain to smart healthcare. In recent years, low-power wireless technologies have come to the forefront as an essential part of efficient HCS built on the IoT. There are also substantial privacy and security concerns addressed. Technologies enabling the rapid group of huge volumes of medical data, such as crowdsourcing as well as crowd sensing, get a lot of attention.

Alzahrani Bander A. [12] detailed the numerous TMIS-based authentication protocols to certify the confidentiality of patient medical data and to validate the identities of all parties involved in TMIS before exchanging sensitive credentials and diagnostic results. Nonetheless, improved and more secure key agreements are still required. Karthegaveni et al. recently demonstrated an elliptic curve cryptography protocol for remote health care monitoring. However, discover that their protocol has a number of weaknesses, such as vulnerabilities to replay attacks, denial-of-service attacks, and a lack of client-server mutual authentication. A number of technical gaps are also in the proposal. A secure and efficient protocol based on TMIS that employs basic symmetric key operations.

Wong et al. [13] highlighted a time-constrained, three-factor quick authentication method that protects user anonymity for multi-server e-health systems operating on 5G-based WSNs. The three-factor authentication method use in work, which combines biometrics, passwords, as well as smart cards, guarantees a high level of security for sensor-enabled environments. While communicating, users' privacy is safeguarded. Furthermore, there are several HC settings that might benefit from time-bound authentication in terms of security.

Awaisi et al. [14] described IoT-based HCS, provide an efficient fog-based architecture. A user authentication technique based on identity management is then to avoid security breaches. To optimize the execution of data from the medical IoT devices and body sensor network, the fog-based architecture for HC incorporates the concept of

virtual machine (VM) partitioning in the fog node. An Elliptic Curve Cryptography method is recycled to produce the user authentication method's output token.

Masood et al. [15] highlighted a privacy-preserving method using multipath routing along with secret key ideas is proposed for healthcare applications that depend on WSNs. Following ECSO's (Enhanced Cuckoo Search Optimization) lead, calculate many sink routes. The method employs distance as a parameter, as well as the route traffic rate, to determine the optimal ECSO pathways. One of these pathways is found to be optimal based on node energy using BO (Butterfly Optimization), which helps reduce the network's energy consumption. Data will be sent encrypted to the sink by means of the particular route.

Bahache et al. [16] applied the absence of data security, malicious actors might alter the data sent via WMSNs, which can lead to disastrous consequences. Consequently, robust authentication protocols and security solutions are necessary. There has been a lot of recent focus on WMSN authentication, with many methods to meet security and privacy standards. There are a lot of performance as well as security issues caused by the few devices recycled in these systems. This research presents the first architecture-based classification of WMSN authentication solutions, as far as aware. The report goes into detail on the authentication methods' security and efficacy.

M. Asassfeh, N. Obeid, and W. Almobaideen [17] provided the best practices for HCS security, with a focus on Anonymous Authentication. It takes a look at these approaches through the lens of the many security threats, safeguards, approaches used to tackle individual security issues, along with network technologies (such WSN and RFID) that were employed. When it comes to security vulnerabilities and security controls, that every plan had certain weaknesses. Security attacks, such as denial of service and change attacks, should get more attention in upcoming study. The same holds true for non-tracking along with backward/forward secrecy as security measures.

3. Proposed Methodology

The ever-developing technology of WSNs has the potential to revolutionise human life. Potential areas for Wireless Medical Sensor Network or WMSN include HC applications, which use medical sensors to monitor patients' health. WMSNs, are the basic technology used in HC applications that allow data collection from biosensors that are worn and measure important body parameters. In order to examine the energy-efficient multipath routing in the context of a privacy-preserving WSNs. To identify multipath search, the following techniques are presented in Elgamal Cryptography Technique for Data EP. The general arrangement of the proposed method as represented in Figure 1.

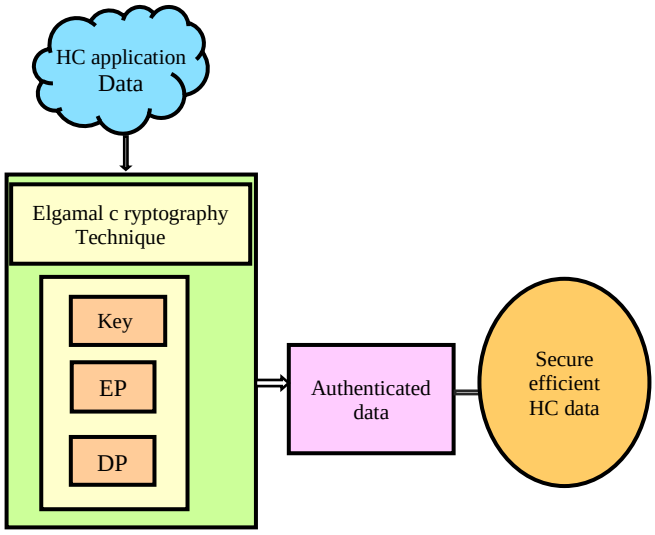

Figure 1. Architecture for Proposed method

3.1. Security Requirement

One of the many different types of software security features may be satisfied by adhering to a set of requirements that outline the essential security functions. Past vulnerabilities, applicable laws, and industry norms all influence security needs. It is impossible to achieve security policy goals without considering all three of the interdependent constraints: (1) confidentiality, (2) integrity, and (3) availability.

a. Confidentiality

In order to keep information's access control and disclosure restrictions in place, make sure that copyrighted information and personal privacy regulations will not be broken.

b. Integrity

In order to forestall the wrong (illegal) alteration or destruction of data. Here, the truthfulness of the information and its non-repudiation are ensured.

c. Availability

The data has to be usable at all times, and dependable access is essential. The truth is that it need only be true for those with access privileges [18].

While effective symmetric-key cryptosystems have been developed and used to secure MWSNs, they may not be able to prevent insider attacks that occur when administrators disclose sensitive patient information. Protecting against inside attacks requires the use of very complex cryptographic techniques, like elgamal EP.

3.2. Registration

Three parts are involved in this system for secure cloud-assisted IoT applications: User (U), Cloud Service Centre (CSC), and Authenticator (A). Any time a user needs to get into the system. In order to access data files in WBAN/IOT,

participants are required to register with the CSC, which will then issue a unique certificate.

a. In order to access or upload a file, user U must first go to the authenticator and get authentication authority.
b. After the user has registered, the Authenticator will verify their identity by uploading encrypted biometric data. If haven't already, go ahead and register to save the details.
c. Redirect user U to CSC after authenticating them.
d. The user is to choose between accessing existing files or uploading a new one. The user will be granted access to a licence that allows them to access certain files for a defined period of time.
e. The authorised user must any files saved in the cloud may be accessed by U.

The importance of security and user privacy protection is growing in relation to the trend of organisations and people outsourcing data storage to the cloud. The main focus of data file EP as well as DP is on the user, ensuring that only authorised users may upload along with download files along with designating whether a file can be shared with other users. When it comes to the topic of data security in the cloud, there are two camps. This research provides the following three-stage framework for the proposed hybrid effort to retain assets in cloud storage.

The four steps of the proposed security approach are as follows: AuthUser, KeyGen, EncryData, and DecryData. The AuthUser step ensures the safe outsourcing of data to the cloud by authenticating the IoT user. The next step in this system is generating a public(PuK) and private key(PrK), and the cloud server runs the KeyGen module to do just that. The data is encrypted by means of the proposed approach as well as stored in a cloud database during the EncryData step. This module decrypts the data using the proposed technique at the time of data retrieval; it is called DecryData [21].

3.3. Cryptographic Elgamal Algorithm

An example of cryptography is a system that uses PuK. Initialization (Key Generation), EP, as well as DP are the three main methods. Access to HC sensing data is provided in this module. App for HC data that can be accessed from any of the three servers. Encrypts the HC data using Elgamal EP with the use of a Elgamal PuK. Using the Elgamal PrK that was generated during Elgamal DP, it then decrypts the HC data that was encrypted before. It seems that EP and DP are handled independently in sensed data, as ElGamal relies on the one-way function. The EP process requires two modular exponentiations [18].

i. Generating Keys:

a. Generate a big, arbitrary prime number (p).
b. Decide on a initiator's identifier(a).
c. Choose an integer (x) less than (p-2), to be secret number.
d. Calculate (d) where d= $d = a^x mod\ p$
e. Choose the PuK(p,a,d) , and the PrK (x).

ii. EP:

a. Acquire the PuK (p,a,d) from the receiver A.
b. Choose an integer k such that:
   - 1<K<p-2
c. Denote the PT in the form of an integer m where
   - 0<m<p-1
d. Total (y) as given: y=a*x mod p
e. Calculate (z) as follows: z= 〖(d〗 *k*m)mod p
f. Acquire the CT (c) as c=(y,z)
g. The sender B transmits C to the receiver A.

iii. DP:

a. Acquire the CT (c) from B.
b. Calculate (r) as below:
   - $r=y^{(p-1-x)}$ mod p
c. Recover the PT as given: m=(r*z)mod p

Initiating the aforementioned parameters is the first stage of the algorithm. For each of these medical records, the procedure is repeated after each of these blocks undergoes EP. In order to avoid potentially large numbers that may arise during the EP process, it is crucial to shorten the data length before EP. As a result, HC data might benefit from the ElGamal algorithm. Here, the number of message blocks will be divided based on the data size, which is the main difference.

The ElGamal algorithm generates private and secret keys for encrypting HC data; it is a PuK EP technique. The administration and security of these keys are thus the main concerns. Using certain hardware modules in conjunction with KM software may provide this level of security. Furthermore, the degree of security that may be achieved is highly dependent on the length of the keys that are used for data EP.

4. RESULTS AND DISCUSSIONS

This section, discuss the results of the proposed security algorithm in the MWSN environment.

4.1. Evaluation metrics

Evaluations of lightCrypt and its rivals using publicly accessible datasets. The assessment uses four metrics: throughput, end-to-end(E2E) latency, Packet Delivery Ratio (PDR) as well as energy consumption, EP time, and attack detection.

4.2. Throughput (Mbyte/sec)

Throughput in WSNs as the number of successfully transported packets per second from source to destination.

An assault significantly lowers the throughput value, which means that it needs to be higher in a well-formed network.

4.3.E2E Delay(ms)

End to End latency is the average amount of time it takes for a packet to go from its source node to its destination node inside a system.

4.4. Packet delivery ratio (per second)

This research calculates PDR and compare it with and without network attack detection. It is clear that the sink node has received fewer packets during the assault since the PDR ratio is much lower than it would be in the absence of the attack.

4.5. EP time (MilliSec)

For any cryptography algorithm, the amount of time it takes to transform PlainText (PT) into CipherText (CT) is known as the EP time. the comparison of throughput metrics for WBAN [21], SCDAM with ECC and lightCrypt-based routing. The graph clearly shows that lightCrypt-based routing outperforms other conventional methods because it applies the energy- and delay-sensitive routing concepts. The current approaches achieve 360 and 350 Mbyte/sec, respectively, whereas the suggested method obtains 370 Mbyte/sec. Figure 6 shows a comparison of the E2E delay values for WBAN, SCDAM with ECC and lightCrypt protocol routing. It is also possible to measure the E2E latency for these nodes in milliseconds (ms), and there are 30–160 of them. Since lightCrypt-based routing reduces the delay factor while searching for suitable routes, it beats other current strategies with low E2E delay, as seen in the graph. In comparison to previous approaches, the suggested ones attain lower 50 (ms) and higher 70 (ms) and 65 (ms), respectively. Pictured in Fig. 2 is a comparison of PDR-based WBAN, SCDAM with ECC and lightCrypt routing. The number of nodes is given in seconds, and it ranges from 30 to 160. It is evident from the graph that lightCrypt -based routing is superior to other modern ways that have improved PDR because of the collective success achieved in terms of the optimum route. The current approach achieves 0.95 percent, whereas the new algorithm reaches 0.85 percent and 0.95 percent, respectively.

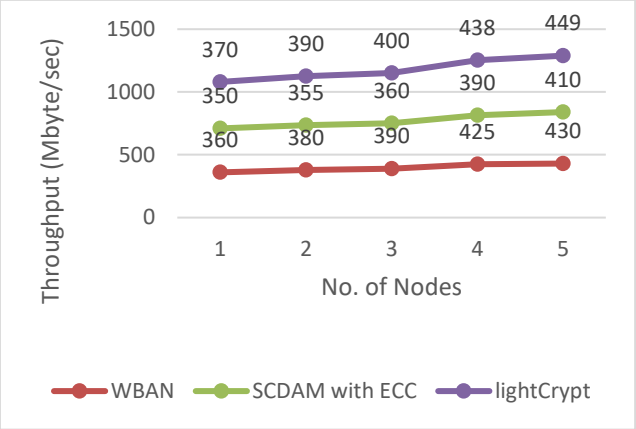

Figure 2. Throughput Results

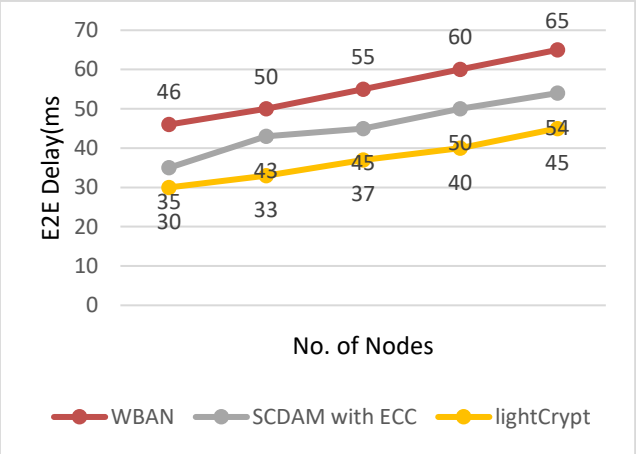

Figure 3. E2E Delay Results

Time use comparisons for lightCrypt, SCDAM with ECC and WBAN rooted routing. The encrypted time, which is specified for individual nodes in milliseconds (Ms), is changing as a result of the movement. The graph verifies that lightCrypt -based routing is superior to other methods that minimise encrypted time usage, thanks to its enhanced residual time. In comparison to current approaches, which reach 170 and 98 milliseconds, respectively, the suggested method finishes in 55 milliseconds, a very short amount of time.

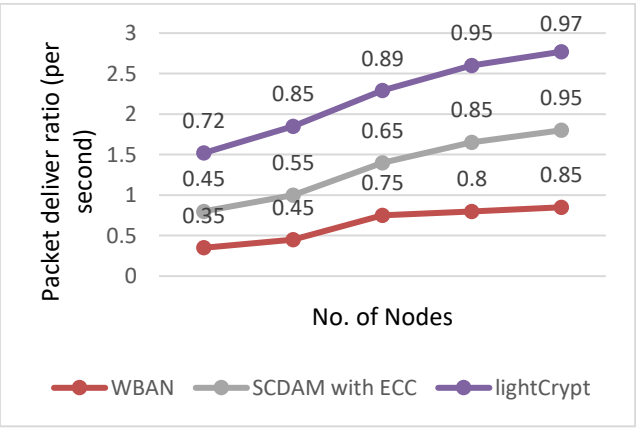

Figure 4. Packet Deliver Ratio Results

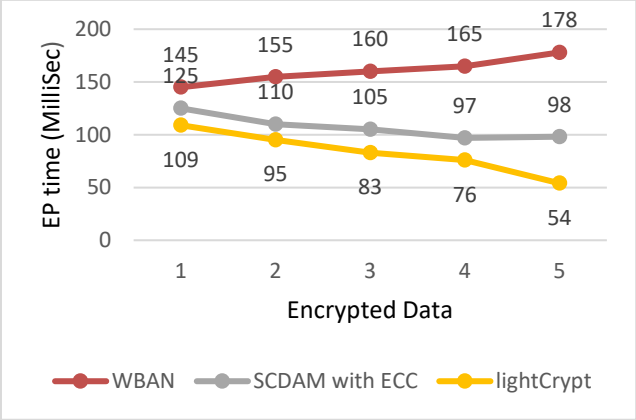

Figure 5. EP time Results

5. CONCLUSION AND FUTURE WORK

A lightweight EP system for WSNs, LightCrypt, is proposed in this work. The proposed method also effectively lowers the EP overhead while having a negligible effect on security. To decrease the computational burden associated with managing cryptographic keys as well as the authentication process between WSN nodes, the proposed strategy also includes a lightweight KM along with authentication technique. The analysis of LightCrypt was conducted by looking at its EP time, power usage, and network lifespan. An examination of the proposed scheme's security reveals that it can withstand common WSN attacks such as brute force, eavesdropping, man-in-the-middle as well as replay attacks. We want to explore the possibility of modifying our proposed strategy for other IoT uses in future studies. IoT security is comparable to that of wireless networks, and it is quickly becoming an important topic. In order to apply and assess our proposed system in actual IoT situations, we may extend the end.

References

[1] Khare, Ankur, Rajendra Gupta, and Piyush Shukla.:Securing IoT Devices for Healthcare Systems Using Optimization-Based Approaches." In IoT in Healthcare Systems, pp. 27-47. CRC Press, (2023).

[2] Pandey, Chetan, Sachin Sharma, and Priya Matta.:Privacy techniques for body sensor network in healthcare internet of things (HIoT)-a critical survey. In 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), pp. 385-389. IEEE, (2021).

[3] Chaudhary, Ravi Raushan Kumar, and Kakali Chatterjee.:An efficient lightweight cryptographic technique for IoT based E-healthcare system. In 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN), pp. 991-995. IEEE, (2020).

[4] Yin, Xiao Chun, Zeng Guang Liu, Bruce Ndibanje, Lewis Nkenyereye, and S. M. Riazul Islam.:An IoT-based anonymous function for security and privacy in healthcare sensor networks. Sensors 19, no. 14 (2019),pp. 3146.

[5] Sureshkumar, Venkatasamy, Ruhul Amin, V. R. Vijaykumar, and S. Raja Sekar.:Robust secure communication protocol for smart healthcare system with FPGA implementation. Future Generation Computer Systems 100 (2019) pp. 938-951.

[6] Sulthana, A. S. R., Ramapati Mishra, Rajesh Singh, Bhasker Pant, Shilpa Sachin Bhojne, and Ch Raghava Prasad. :Wireless Sensor Networks Face Challenges and Issues Related to Security. In 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 943-949. IEEE, (2023).

[7] Jan, Saeed Ullah, Anwar Ghani, Abdulrahman Alzahrani, Syed Muhammad Saqlain, Khalid Yahya, and Haseeb Sajjad.:Bandwidth and Power Efficient Lightweight Authentication Scheme for Healthcare Systeme. Journal of King Saud University-Computer and Information Sciences (2023),pp.101601.

[8] Kasyoka, Philemon Nthenge, Michael Kimwele, and Shem Angolo Mbandu.:Efficient certificateless signcryption scheme for wireless sensor networks in ubiquitous healthcare systems. Wireless Personal Communications 118 (2021), pp. 3349-3366.

[9] Jabeen, Tallat, Ishrat Jabeen, Humaira Ashraf, N. Z. Jhanjhi, Abdulsalam Yassine, and M. Shamim Hossain.:An Intelligent Healthcare System Using IoT in Wireless Sensor Network. Sensors 23, no. 11 (2023),pp. 5055.

[10] Huang, Haiping, Tianhe Gong, Ning Ye, Ruchuan Wang, and Yi Dou. :Private and secured medical data transmission and analysis for wireless sensing healthcare system. IEEE Transactions on Industrial Informatics 13, no. 3 (2017), pp. 1227-1237.

[11] Gardašević, Gordana, Konstantinos Katzis, Dragana Bajić, and Lazar Berbakov. :Emerging wireless sensor networks and Internet of Things technologies—Foundations of smart healthcare. Sensors 20, no. 13 (2020), pp. 3619.

[12] Alzahrani, Bander A. :Secure and efficient cloud-based IoT authenticated key agreement scheme for e-health wireless sensor networks. Arabian Journal for Science and Engineering 46, no. 4 (2021),pp. 3017-3032.

[13] Wong, Alice May-Kuen, Chien-Lung Hsu, Tuan-Vinh Le, Mei-Chen Hsieh, and Tzu-Wei Lin :Three-factor fast authentication scheme with time bound and user anonymity for multi-server E-health systems in 5G-based wireless sensor networks. Sensors 20, no. 9 (2020),pp. 2511.

[14] Awaisi, Kamran Sattar, Shahid Hussain, Mansoor Ahmed, Arif Ali Khan, and Ghufran Ahmed. :Leveraging IoT and fog computing in healthcare

systems. IEEE Internet of Things Magazine 3, no. 2 (2020),pp. 52-56.
[15] Masood, Jafar Ali Ibrahim Syed, M. Jeyaselvi, N. Senthamarai, S. Koteswari, M. Sathya, and NS Kalyan Chakravarthy. :Privacy preservation in wireless sensor network using energy efficient multipath routing for healthcare data. Measurement: Sensors 29 (2023),pp. 100867.
[16] Bahache, Anwar Noureddine, Noureddine Chikouche, and Fares Mezrag.:Authentication schemes for healthcare applications using wireless medical sensor networks: A survey. SN Computer Science 3, no. 5 (2022),pp. 382.
[17] Asassfeh, M., Nadim Obeid, and Wesam Almobaideen.:Anonymous authentication protocols for iot based-healthcare systems: a survey. International Journal of Communication Networks and Information Security 12, no. 3 (2020),pp. 302-315.
[18] Masood, Jafar Ali Ibrahim Syed, M. Jeyaselvi, N. Senthamarai, S. Koteswari, M. Sathya, and NS Kalyan Chakravarthy. "Privacy preservation in wireless sensor network using energy efficient multipath routing for healthcare data." Measurement: Sensors 29 (2023): 100867.
[19] Khashan, Osama A., Rami Ahmad, and Nour M. Khafajah. "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks." Ad Hoc Networks 115 (2021): 102448.
[20] Bhavani, A., and V. Nithya. "Cryptographic algorithm for enhancing data security in wireless IoT sensor networks." Intelligent Automation & Soft Computing 36, no. 2 (2023): 1381-1393.
[21] Shrivastava, Vineeta, and Mayank Namdev. "Secure Elgamal Based Authentication Scheme for Cloud Assisted IOT Based Wireless Body Area Network."

Authors Contributions

Ms.Sangeetha Komandur[1]: Conceptualization, Investigation,

Visualization

Ms.Sameena Shaik[2] : Writing original draft preparation:Writing,

reviewing and editing.

Conflicts of Interest

The authors declare no conflicts of interest